

Remarks

With respect to the rejection of claims 1, 2, 10, 11, 19 and 21-23 under 35 U.S.C. § 102 (b), the Examiner has attempted to identify in Landfield those structures or functions that correspond to each of the limitations in Applicants' claims. In this regard, Applicants respectfully submit that the Examiner has either misinterpreted the language of Applicants' claims or misunderstood the cited reference. As a result, Applicants believe that the Examiner has failed to establish anticipation.

1. As set forth in claim 1, lines 1-3, Applicants' system is expressly designed "to *prevent* transfer of selected communication transactions from an untrustworthy network [e.g., a public network] to a trustworthy network [e.g., a private network] ... " (emphasis added). In contrast, the Landfield system is expressly designed to *allow* electronic mail inbound from a public network to reach the appropriate users of a private network (see, Landfield, col. 2, lines 60-64). In the case of the Applicants' system, the protection rules are **exclusive**, that is, each rule defines parameters that, if met, will result in the exclusion of the transaction, whereas in the event the parameters are not met, the transaction will be allowed. In the case of the Landfield system, the aliases in the local alias database are **permissive**, that is, each alias defines parameters that, if met, will result in the allowance of the transaction, whereas in the event the parameters are not met, the transaction will be prevented. Thus, the Applicants' system, *as claimed*, operates precisely opposite from the system disclosed in Landfield. According, Applicants respectfully submit that the rejections of claim 1 and its dependent claim 2 are improper.

2. As set forth in claim 10, lines 1-3, Applicants' method is expressly designed "to *prevent* transfer of selected communication transactions from an untrustworthy network [e.g., a public network] to a trustworthy network [e.g., a private network] ... " (emphasis added). In contrast, the method practiced by the Landfield system is expressly designed to *allow* electronic mail inbound from the public network to reach the appropriate users of the private network (see, Landfield, col. 2, lines 60-64). In the case of the Applicants' method, the protection rules are **exclusive**, that is, each rule defines parameters that, if met, will result in the exclusion of the transaction, whereas in the event the parameters are not met, the transaction will be allowed. In the case of the Landfield method, the aliases in the local alias database are **permissive**, that is, each alias defines parameters that, if met, will result in the allowance of the transaction, whereas in the event the parameters are not met, the transaction will be prevented. Thus, the Applicants' method, *as claimed*, operates precisely opposite from the method disclosed in Landfield. According, Applicants respectfully submit that the rejections of claim 10 and its dependent claim 11 are improper.

3. As set forth in claim 19, lines 1-3, Applicants' portal is expressly designed "to *prevent* transfer of selected communication transactions from an untrustworthy network [e.g., a public network] to a trustworthy

network [e.g., a private network] ... " (emphasis added). In contrast, the Landfield firewall host system 28 is expressly designed to *allow* electronic mail inbound from the public network to reach the appropriate users of the private network (see, Landfield, col. 2, lines 60-64). In the case of the Applicants' portal, the protection rules are **exclusive**, that is, each rule defines parameters that, if met, will result in the exclusion of the transaction, whereas in the event the parameters are not met, the transaction will be allowed. In the case of the Landfield firewall host system 28, the aliases in the local alias database are **permissive**, that is, each alias defines parameters that, if met, will result in the allowance of the transaction, whereas in the event the parameters are not met, the transaction will be prevented. Thus, the Applicants' portal, *as claimed*, operates precisely opposite from the firewall host 28 disclosed in Landfield. According, Applicants respectfully submit that the rejection of claim 19 is improper.

4. As set forth in claim 21, lines 1-3, Applicants' system is expressly designed "to *prevent* transfer of selected communication transactions from an untrustworthy network [e.g., a public network] to a trustworthy network [e.g., a private network] ... " (emphasis added). In contrast, the Landfield system is expressly designed to *allow* electronic mail inbound from the public network to reach the appropriate users of the private network (see, Landfield, col. 2, lines 60-64). In the case of the Applicants' system, the protection rules are **exclusive**, that is, each rule defines parameters that, if met, will result in the exclusion of the transaction, whereas in the event the parameters are not met, the transaction will be allowed. In the case of the Landfield system, the aliases in the local alias database are **permissive**, that is, each alias defines parameters that, if met, will result in the allowance of the transaction, whereas in the event the parameters are not met, the transaction will be prevented. Thus, the Applicants' system, *as claimed*, operates precisely opposite from the system disclosed in Landfield. According, Applicants respectfully submit that the rejection of claim 21 is improper.

5. As set forth in claim 22, Applicants' portal is expressly designed "to selectively transfer a communication transaction" (lines 1-3) by "*preventing* the transfer of the communication transaction if required by the protection rule" (lines 7-8)(emphasis added). In contrast, the Landfield firewall host system is expressly designed to *allow* electronic mail inbound from the public network to reach the appropriate users of the private network (see, Landfield, col. 2, lines 60-64). In the case of the Applicants' portal, the protection rules are **exclusive**, that is, each rule defines parameters that, if met, will result in the exclusion of the transaction, whereas in the event the parameters are not met, the transaction will be allowed. In the case of the Landfield firewall host system, the aliases in the local alias database are **permissive**, that is, each alias defines parameters that, if met, will result in the allowance of the transaction, whereas in the event the parameters are not met, the transaction will be prevented. Thus, the Applicants' portal, *as claimed*, operates precisely opposite from the firewall system disclosed in Landfield. Furthermore, Applicants can find no

teaching or suggestion in Landfield that the firewall host system 28 can "selectively [transfer] to the [firewall host system 26] at least a portion of the received [email] even if the protection rule allows transfer of the received [email]" (lines 9-11). Indeed, since, in Landfield, the transfer would be allowed only if there was a respective permissive rule in the alias database, it would make no sense for firewall host system 28 to report *valid* email traffic to firewall host system 26. According, Applicants respectfully submit that the rejection of claim 22 is improper.

6. In the method of claim 23, Applicants' portal "selectively transfers a communication transaction" (lines 1-3) by "*preventing* ... the transfer of the communication transaction if required by the first protection rule" (lines 8-9)(emphasis added). In contrast, the Landfield firewall host system 28 is expressly designed to *allow* electronic mail inbound from the public network to reach the appropriate users of the private network (see, Landfield, col. 2, lines 60-64). In the case of the Applicants' portal, the protection rules are **exclusive**, that is, each rule defines parameters that, if met, will result in the exclusion of the transaction, whereas in the event the parameters are not met, the transaction will be allowed. In the case of the Landfield firewall host system 28, the aliases in the local alias database are **permissive**, that is, each alias defines parameters that, if met, will result in the allowance of the transaction, whereas in the event the parameters are not met, the transaction will be rejected. Thus, the Applicants' portal, *as claimed*, operates precisely opposite from the firewall host system 28 disclosed in Landfield. Furthermore, Applicants can find no teaching or suggestion in Landfield that the firewall host system 28 can "selectively [transfer] from [itself] to the [firewall host system 26] at least a portion of the [email] even if the first [alias] allows transfer of the [email]" (lines 10-12). Indeed, since, in Landfield, the transfer would be allowed only if there was a respective alias in the alias database, it would make no sense for firewall host system 28 to send portions of *valid* emails to firewall host system 26. Finally, assuming *arguendo* that such functionality was either taught or suggested in Landfield, Applicants can find no teaching or suggestion in Landfield that the firewall host system 26 is capable of "selectively creating ... a second [alias] in response to [the portion of the email that we have assumed was sent by firewall host system 28]" (lines 13-14). According, Applicants respectfully submit that the rejection of claim 23 is improper.


In the present Office Action, the Examiner has noted that Applicants' arguments as set forth in the Amendment filed 22 February 2005 were not persuasive with respect to the Examiner's previous rejection of claim 20 as being unpatentable over Nessett in view of Sheldon as set forth in the Office Action of 10 February 2004. In particular, the Examiner has pointed out that, as presently claimed, it is not sufficiently clear that the server selectively transfers the protection rules to the portal via the untrustworthy network *at the request of the portal* and not as a result of a decision to do so independently made by the server. In order to more particularly point out and distinctly claim this aspect of Applicants' portal, Applicants have amended claim 20 (as set forth above) such that it is now clear that the server transfers to the portal the protection rules

database "upon request by the portal" (see, claim 20, line 8). In view of this amendment, Applicants respectfully submit that claim 20 now patentably distinguishes over Nessett, even in view of Sheldon, for the purposes of 35 U.S.C. § 103 (a).

Conclusion:

Applicants respectfully request entry of the amendment proposed hereinabove. Further, Applicants respectfully submit that claims 1-23, as may be amended herein, are all allowable over the cited art. Therefore, in the belief that we have responded to each and every rejection contained in the Office Action of 18 May 2005, Applicants respectfully request reconsideration and allowance of claims 1-23.

Respectfully submitted,
Stuart D. Green, *et al.*



Jeffrey Van Myers
Attorney for Applicants
Reg. No. 27,362
Ph: 512.858.7453